**UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**
**EASTERN DIVISION**

VERNITA MIRACLE-POND and SAMANTHA PARAF, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

SHUTTERFLY, INC.,

Defendant.

Civil Action No. 1:19-cv-4722

District Judge Mary M. Rowland

# MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

MAYER BROWN LLP
Lauren R. Goldman
Michael Rayfield*
1221 Avenue of the Americas
New York, NY 10020
Telephone: (212) 506-2500
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

John Nadolenco* (*pro hac vice*)
350 South Grand Avenue
25th Floor
Los Angeles, CA 90071
Telephone: (213) 229-9500
jnadolenco@mayerbrown.com

*Attorneys for Defendant Shutterfly, Inc.*
**pro hac vice* application to be filed

# TABLE OF CONTENTS

**Page**

## TABLE OF AUTHORITIES

**Page(s)**

**Cases**

**Statutes**



**Other Authorities**

## INTRODUCTION

This is the third iteration of the same meritless lawsuit brought by the same law firm. Shutterfly is a manufacturer and digital retailer of personalized products and services. Its services include free online tools that allow people to upload, organize, and share digital photographs in a centralized, easily accessible location. To make it easier for users to organize their photos, Shutterfly uses facial-recognition technology to analyze uploaded photos, and then employs information derived from that analysis to "group" photos together that may contain the same face—the user's friend or family member, for example. The user then has the option to "tag" that group with a label of his own choice, *e.g.*, "Jane," "Mom," or "Uncle Joe."

Plaintiffs challenge this helpful feature by invoking an Illinois statute that has no connection to the technology at issue. Vernita Miracle-Pond alleges that she has a Shutterfly account; Samantha Paraf alleges that she has never had an account.[1] Both allege that their faces appear in photographs uploaded to the service by unidentified Shutterfly users in Illinois, and that without their consent, Shutterfly then used facial-recognition technology to extract "biometric identifiers" from the photos for the purpose of suggesting tags to users. Plaintiffs claim that this violated the Illinois Biometric Information Privacy Act ("BIPA"), a statute enacted in 2008 to regulate the use of biometric technologies (like retina scans and fingerprints) in connection with financial transactions and security screenings occurring in this State.

The suit lacks merit for numerous reasons, at least two of which appear on the face of the complaint. First, BIPA applies only to "biometric identifiers" and "biometric information," and expressly defines those terms to *exclude* "photographs" and any "information derived from" photographs. Because plaintiffs' claim is based entirely on Shutterfly's alleged extraction of

[1] Shutterfly has concurrently filed a motion to compel arbitration as to Ms. Miracle-Pond. Ms. Miracle-Pond agreed to Shutterfly's terms of service, which include an arbitration clause. This motion to dismiss is filed in the alternative as to Ms. Miracle-Pond.

information from photographs, it fails. We acknowledge that several district courts have previously held—for different reasons—that BIPA's photograph exception did not require the dismissal of complaints based on the application of facial recognition-technology to online photos, including in the two previous cases filed against Shutterfly. We respectfully submit, however, that this Court should not follow those decisions. As explained below, they do not properly account for the plain meaning of BIPA's text, structure, and legislative history—all of which make clear that BIPA was not intended to impose liability in this context.

Second, this Court should at minimum dismiss plaintiffs' allegation that Shutterfly violates BIPA by "selling, leasing, trading, or otherwise profiting from Plaintiffs' and Class members' biometric identifiers and/or biometric information." Plaintiffs have simply offered "no factual detail" at all "to support these conclusory allegations," as required by *Twombly* and *Iqbal*. *Yeftich v. Navistar, Inc.*, 722 F.3d 911, 916 (7th Cir. 2013).

## BACKGROUND

### A. The Illinois Biometric Information Privacy Act

BIPA was enacted in 2008 to address the growing use of biometric data "in the *business and security screening sectors*" in Illinois. 740 ILCS 14/5(a) (emphasis added). The Illinois General Assembly found that "[t]he use of biometrics is growing in [these] sectors and appears to promise streamlined financial transactions and security screenings" (*id.*), including purchases powered by "finger-scan technologies at grocery stores, gas stations, and school cafeterias" (*id.* 14/5(b)). But because there is a "heightened risk for identity theft" when biometric data is "compromised" (*id.* 14/5(c)), "many members of the public [had been] deterred from partaking in biometric identifier-facilitated transactions" (*id.* 14/5(e)). The legislature found that the public would "be served by regulating" this data under certain circumstances. *Id.* 14/5(g).

BIPA addresses these concerns by regulating the collection and storage of (1) "biometric identifiers" and (2) "biometric information." *Id.* 14/10. The statute defines "biometric identifier" as a short, exclusive list of sources of data about a person: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." *Id.* Other potential identifiers, including "photographs," are then expressly excluded from the definition. *Id.*

"Biometric information" is data derived from a biometric identifier: "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.* This provision, too, contains an exclusionary clause: "Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers"—such as "photographs." *Id.* Thus, both "photographs" and "information derived from" photographs are removed from BIPA's coverage.

Private entities that collect biometric data must comply with five requirements: They must publish a written "schedule and guidelines" for the retention and destruction of the data. *Id.* 14/15(a). They must inform the subject "in writing" of the collection, the purpose, and the duration of storage, and obtain a "written release" before collecting the data. *Id.* 14/15(b). They may not "sell, lease, trade, or otherwise profit" from the data. *Id.* 14/15(c). They may not "disclose" or "disseminate" the data without consent. *Id.* 14/15(d). And they must take reasonable measures to "protect from disclosure" all regulated data. *Id.* 14/15(e).

BIPA provides a "right of action" to "[a]ny person aggrieved by a violation of this Act." *Id.* 14/20. A plaintiff may recover "liquidated damages of $1,000 or actual damages, whichever is greater," but only if he proves that the defendant "negligently" violated BIPA; if the defendant "intentionally or recklessly" violated BIPA, the plaintiff may recover "liquidated damages of $5,000 or actual damages, whichever is greater." *Id.* 14/20(1)-(2).

**B. Prior BIPA Lawsuits Against Shutterfly**

In June 2015, a different plaintiff represented by the same counsel filed a BIPA lawsuit against Shutterfly in this District. *Norberg v. Shutterfly, Inc.*, No. 15-cv-05351 (N.D. Ill. 2015). Judge Norgle denied Shutterfly's motion to dismiss. *Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103 (N.D. Ill. 2015). Shutterfly then filed a motion to compel arbitration based on public information indicating that the photo at issue had been uploaded by the plaintiff's wife, a Shutterfly user bound by an arbitration clause. *See Norberg* Dkt. 79. The case settled three weeks later and was dismissed with prejudice. *See Norberg* Dkts. 89, 91.

The same counsel then found another plaintiff—who was neither a Shutterfly user nor an Illinois resident—to file a BIPA lawsuit against Shutterfly on November 30, 2016. *Monroy v. Shutterfly*, No. 16-cv-10984 (N.D. Ill. 2016). Judge Gottschall denied Shutterfly's motion to dismiss. *Monroy v. Shutterfly*, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017). After discovery revealed that the photo on which the plaintiff's claim was based was not uploaded from Illinois, the parties stipulated to a dismissal of the case with prejudice. *Monroy* Dkt. 106.

**C. Plaintiffs' Claims**

Just two months later, the two plaintiffs here filed the operative complaint through the same counsel. One plaintiff (Ms. Miracle-Pond) is a user of Shutterfly, and the other (Ms. Paraf) is a non-user. Compl. (Dkt. 1) ¶¶ 7-8. Both claim to be Illinois residents. *Id.* Plaintiffs allege that Shutterfly uses facial-recognition software to "extract[], collect[], and store[] millions of 'scans of face geometry'—highly detailed geometric maps of the face—from every individual who appears in a photograph uploaded to Shutterfly," and that these "scans" are "biometric identifiers" under BIPA. *Id.* ¶¶ 5, 23, 24, 26. They claim Shutterfly uses this data to suggest tags for faces in uploaded photographs that match "scans of face geometry already saved in Shutterfly's face database." *Id.* ¶ 25. Plaintiffs allege that "[t]hese unique biometric identifiers

are not only collected and used by Shutterfly to identify individuals by name, but also to recognize their gender, age, race and location," and that Shutterfly thereby collects "'biometric information' from individuals appearing in user-uploaded photos." *Id.* ¶ 26.

Plaintiffs allege that their "face[s] appear[] in photographs uploaded to Shutterfly within Illinois," but do not say when those photos were uploaded or who uploaded them. *Id.* ¶¶ 7-8. Nor do they allege that they were tagged in any of those photos. They claim that, "[u]pon upload of the photographs," Shutterfly applied facial-recognition technology to the photos without complying with BIPA's notice-and-consent provisions. *Id.* ¶¶ 29-33. They further allege, "[u]pon information and belief," that "Shutterfly is selling, leasing, trading, or otherwise profiting from Plaintiffs' and Class members' biometric identifiers and/or biometric information." *Id.* ¶ 48. Plaintiffs seek to represent a putative class of "[a]ll Illinois citizens who had their biometric identifiers, including scans of face geometry and related biometric information, collected, captured, received, or otherwise obtained by Shutterfly from photographs uploaded to Shutterfly within the state of Illinois." *Id.* ¶ 34.

## ARGUMENT

Plaintiffs' entire complaint is barred by BIPA's photo exception. If the Court concludes that plaintiffs can state a claim under BIPA's notice-and-consent provisions, it should dismiss their claims under BIPA's provisions governing the disclosure and sale of biometric data.[2]

### I. BIPA DOES NOT APPLY TO SHUTTERFLY'S TECHNOLOGY.

#### A. BIPA Excludes "Information Derived From" Photographs.

Plaintiffs' case rests entirely on data allegedly "extracted" from "photos [that] are uploaded to Shutterfly from within the state of Illinois." Compl. ¶¶ 5, 7-8, 27-33, 42. BIPA's

[2] "A motion to dismiss should be granted if the plaintiff fails to offer 'enough facts to state a claim to relief that is plausible on its face.'" *Ennenga v. Starns*, 2012 WL 1899331, at *2 (N.D. Ill. May 23, 2012) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

definition of "biometric identifier" expressly excludes "photographs," and its definition of "biometric information" excludes "information derived from items or procedures excluded under the definition of biometric identifiers," including photographs. 740 ILCS 14/10. Plaintiffs nonetheless allege that Shutterfly's technology is regulated by the statute, claiming that Shutterfly obtains and stores "scans of face geometry" within the statutory definition of "biometric identifier." Compl. ¶ 5.

Plaintiffs do not mention BIPA's photo exception in their complaint. But their complaint appears to suggest that because information derived from photos is not expressly excluded from the definition of *biometric identifier*, Shutterfly's facial-recognition analysis may be regulated under *that* provision. That is wrong: *All* data "derived from" "photographs" is excluded from BIPA's reach; recharacterizing such data as a "scan of face geometry" does not bring it within the scope of the statute. If the legislature wanted to regulate data derived from photos, it would not have expressly excluded such data from the definition of "biometric information." It would make no sense to exclude this category of data from the definition of "biometric information" but permit it to be regulated as a "biometric identifier," because biometric identifiers and biometric information are subject to all of the same requirements under BIPA. 740 ILCS 14/15. And the legislature did not also *need* to exclude "information derived from" "photographs" from the definition of "biometric identifier," because (as we next discuss) derivative data is not covered by that definition in the first place.

BIPA regulates *two* distinct categories of biometric data: (1) original sources of information about a person ("biometric identifiers"—defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry"); and (2) data derived from those sources ("biometric information"—defined as "information . . . based on an individual's biometric

identifier"). If data "extracted" (Compl. ¶ 42) from photographs were covered by BIPA, it could be regulated only as "biometric information." But it is not; as discussed above, "information derived from" photographs is expressly excluded from the definition of "biometric information." 740 ILCS 14/10. Permitting plaintiffs to force data "extracted" from photos into the *first* category of biometric data—biometric *identifiers*—would nullify the legislature's careful decision to exclude *both* photographs *and* all information derived from them.

The enumerated list of "biometric identifiers" in BIPA provides further evidence that the legislature did not intend the term "scan of face geometry" to cover the application of facial-recognition technology to online photographs. Every item on BIPA's list of "biometric identifiers" is a physical, *in-person* process for obtaining information about an individual that can be used to authenticate a transaction or access a secure area. A "retina scan" involves a live person holding his eye to a specialized machine.[3] A "fingerprint" is produced when a live person touches a card, console, or other object.[4] A "voiceprint" is the product of a live person's spoken words.[5] And most notably, a "scan of hand geometry"—the statutory term closest to "scan of face geometry"—can be accomplished *only* in person: A person's actual hand "is placed on [a]

---

[3] *See* Rawlson King, *Explainer: Retinal Scan Technology*, BiometricUpdate.com (Aug. 30, 2013), http://www.biometricupdate.com/201307/explainer-retinal-scan-technology ("A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece.").

[4] *See* FBI, *Recording Legible Fingerprints*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/recording-legible-fingerprints ("[f]ingerprints can be recorded" either with ink on a "standard fingerprint card" or "electronically using a *live* scan device" (emphasis added)).

[5] *See* Lisa Myers, *An Explanation of Voice Biometrics*, SANS Institute, at 4 (July 24, 2004), https://www.sans.org/reading-room/whitepapers/authentication/exploration-voicebiometrics-1436 ("[t]he user is asked to speak a certain set of words or phrases, or to speak for a certain length of time," and "[f]rom that sample, a digital representation of the voice, called a voiceprint, is created").

plate, palm down, and guided by five pegs that sense when the hand is in place," and then a camera "capture[s] a silhouette image of the hand."[6]

If the application of facial-recognition to online photos constituted a "scan of face geometry" within the meaning of BIPA, that term would have to be categorically different from every other item on the list of biometric identifiers. But "[i]t is a "commonsense canon" of construction that the meaning of a term is "narrowed by . . . the neighboring words with which it is associated," *United States v. Williams*, 553 U.S. 285, 294 (2008), and that one should "avoid ascribing to one [term] a meaning so broad that it is inconsistent with its accompanying words," *People v. Qualls*, 365 Ill. App. 3d 1015, 1020 (2006). That is particularly true of terms grouped in a statutory list: "when a statute contains a list, each word in that list presumptively has a similar meaning." *Yates v. United States*, 135 S. Ct. 1074, 1089 (2015) (Alito, J., concurring) (citing *Gustafson v. Alloyd Co.*, 513 U.S. 561, 576 (1995)).

Thus, in BIPA, the term "scan of face geometry" means an *in-person* scan of a person's *actual* face—not the application of facial-recognition software to an ordinary photo. It includes, for example, "depth images" of faces (also known as 3D face scans) created by scanning someone's face in person using a specialized device, like the iPhone X's TrueDepth Camera.[7] The definition does not apply to the application of facial recognition on online photos.

---

[6] Stephen Mayhew, *Explainer: Hand Geometry Recognition*, BiometricUpdate.com (June 22, 2012), https://www.biometricupdate.com/201206/explainer-hand-geometry-recognition.

[7] *See* Apple, Face ID Security (Nov. 2017), *available at* https://images.apple.com/business/docs/FaceID_Security_Guide.pdf ("Once it confirms the presence of an attentive face, the TrueDepth camera projects and reads over 30,000 infrared dots to form a depth map of the face, along with a 2D infrared image. This data is used to create a sequence of 2D images and depth maps, which are digitally signed and sent to the Secure Enclave.").

### B. BIPA's Legislative Findings And History Confirm That The Statute Was Not Intended To Regulate Data Derived From Online Photographs.

The General Assembly's legislative findings demonstrate that the exclusion of both photos and information derived from them was deliberate. BIPA was designed to regulate the live, in-person use of biometric technologies in connection with "financial transactions and security screenings," 740 ILCS 14/5(a)—not the application of facial-recognition software to photographs. The legislature believed that the increasing use of "biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias," would have a "streamlin[ing]" effect on Illinois commerce. *Id.* 14/5(a), (b). But it anticipated that the "limited State law" in this area would create identity-theft concerns, "deterr[ing] [consumers] from partaking in biometric identifier-facilitated transactions" and perhaps causing them to "withdraw" from such "transactions" altogether. *Id.* 14/5(c), (e). There is no indication in the legislative findings that the General Assembly wanted to regulate companies that apply facial-recognition technology to ordinary photos voluntarily uploaded to social media.

The legislative history confirms BIPA's limited purpose. As BIPA moved toward passage, the definitions of "biometric identifier" and "biometric information" were sharply narrowed. The first Senate version defined "biometric identifier" broadly: "Examples of biometric identifiers *include, but are not limited to*[,] iris or retinal scans, fingerprints, voiceprints, and *records* of hand or facial geometry." Sen. Bill 2400, § 10 (Feb. 14, 2008) (Ex. A) (emphases added). And although the definition of "biometric identifier" always excluded "photographs," the original definition of "biometric information" did *not* exclude information derived from photographs. *Id.* The next proposal was even broader: "biometric identifier" included "records or scans of hand geometry, facial geometry, or *facial recognition*."

Sen. Am. to Sen. Bill 2400, § 10 (Apr. 11, 2008) (Ex. B) (emphasis added). But that proposal was rejected, and the House offered a version that was substantially narrower than the original: It (a) changed the definition of "biometric identifiers" from an open-ended set of "[e]xamples" to a narrow list of enumerated sources; (b) removed the broad term "records" of hand or face geometry; and (c) excluded from the definition of "biometric information" all "information derived from items or procedures excluded under the definition of biometric identifiers." House Am. to Sen. Bill 2400, § 10 (May 28, 2008) (Ex. C). This version was enacted.

In sum, consistent with its findings, the legislature expressly declined to include a "record" of facial geometry in the definition of biometric identifier; to regulate all forms of "facial recognition"; or to allow information derived from photographs to slip into the definition of "biometric information." This history reflects a clear intent to regulate only a narrow set of technologies—and to exclude a host of others, including all forms of facial recognition that are derived from photographs.

### C. The Court Should Not Follow The District Court Decisions That Have Addressed This Issue.

BIPA's photo exception has not yet been construed by the Illinois state courts or by the Seventh Circuit. But four district courts have rejected motions to dismiss BIPA claims based on this exception—for different reasons and with varying degrees of analysis. Shutterfly respectfully submits that those decisions were mistaken, and this Court should not follow them.

***Norberg.*** Shutterfly moved to dismiss the first BIPA case brought by opposing counsel based on the photo exception. Judge Norgle denied that motion in a one-paragraph analysis:

> Here, Plaintiff alleges that Defendants are using his personal face pattern to recognize and identify Plaintiff in photographs posted to Websites. Plaintiff avers that he is not now nor has even been a user of [the] Websites, and that he was not presented with a written biometrics policy nor has he consented to have his biometric

> identifiers used by Defendants. As a result, the Court finds that Plaintiff has plausibly stated a claim for relief under the BIPA.

152 F. Supp. 3d at 1106. The court did not attempt to square the operation of Shutterfly's technology with BIPA's exclusion of photos and information derived from them.

***Facebook Biometric.*** In *In re Facebook Biometric Biometric Information Privacy Litigation*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016), a California federal court held that BIPA's use of the term "'[p]hotographs' is better understood to mean *paper prints* of photographs, not digitized images stored as a computer file and uploaded to the Internet." *Id.* (emphasis added). This interpretation is implausible: BIPA was enacted in ***2008***. "[U]nless otherwise defined," words are given their "contemporary" meaning. *Perrin v. United States*, 444 U.S. 37, 42 (1979). BIPA does not distinguish between paper and digital photos. By 2008, digital photography was the norm: As a 2007 article explains, "[d]igital photography entered the mainstream of consumer consciousness soon after the start of the new century"; "four in five cameras sold in 2005 were digital." Jeremiah A. Armstrong, *The Digital Era of Photography Requires Streamlined Licensing and Rights Management*, 47 Santa Clara L. Rev. 785, 785 (2007). BIPA's reference to "photographs" necessarily encompassed both paper and digital images.[8]

***Rivera.*** In *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088 (N.D. Ill. 2017), a court in this Circuit denied Google's motion to dismiss a BIPA claim based on the photo exception. *Id.* at 1092-1100. The court rejected the *Facebook Biometric* court's "paper prints" rationale. *See id.* at 1095 n.7. It instead held that information derived from photographs is excluded from the term "biometric information" but *not* from the term "biometric identifier"; accordingly, the plaintiff's allegation that Google's technology captured a "scan of face geometry" was enough to state a

[8] *See also* WEBSTER'S DICTIONARY 373 (2008 ed.) (Ex. D) ("photography" means "the art or process of producing images on a sensitive surface (as film or a CCD chip [a form of technology commonly used in digital imaging])").

claim, even though it was undisputed that the alleged "scan" was derived from photographs. *Id.* at 1100. *Rivera*'s analysis is flawed; it rests on the assumption that BIPA lacks a coherent structure and that no meaning can be ascribed to the General Assembly's choices about what to regulate and what to exclude. This Court should not follow it.

As a threshold matter, the *Rivera* court later held that it lacked subject matter jurisdiction, 366 F. Supp. 3d 998, 1014 (N.D. Ill. 2018)—"render[ing] everything that ha[d] occurred" in the litigation "a nullity." *Hart v. Terminex Int'l*, 336 F.3d 541, 541-42 (7th Cir. 2003).

And in any event, the court appears to have misunderstood Google's argument. Like Shutterfly here, Google argued that BIPA's definitions of biometric identifier and biometric information regulate different things: data that "is derived from a *person* is a biometric identifier," whereas data that is "subsequently derived from a *biometric identifier* is biometric information.'" 238 F. Supp. 3d at 1096 (quotation marks omitted; emphasis added). The court rejected this argument on the ground that the statutory definitions do not have a "parallel structure": "The definition of 'biometric identifier' does *not* use words like 'derived from a person,' . . . whereas the definition of 'biometric information' does say that it is information 'based on' a biometric identifier." *Id.* at 1096-07 But Google's argument (like ours here) was that the two definitions are *not* parallel—which is exactly why "biometric identifier" is limited to original sources, and "biometric information" is limited to data extracted or derived from those sources.

The court then found that no "structural meaning" can be drawn from the legislature's decision to exclude a number of items, including photographs, from the definition of "biometric identifier," because those exclusions "comprise a mix of things that are true exceptions . . . and others that read more like just-to-be-sure exclusions." 238 F. Supp. 3d at 1097. That is not a

sound basis to ignore the legislature's deliberate exclusion of information derived from photos from BIPA's only category that encompasses derivative data. The very concept of a statutory provision that is enacted "just to be sure" is anathema to the established principle that a statute must be interpreted to give every term "independent effect." *Devoney v. Ret. Bd. of Policemen's Annuity & Ben. Fund for City of Chicago*, 199 Ill. 2d 414, 420 (2002).

Finally, in rejecting Google's argument that the term "scan of face geometry" refers to an in-person scan of someone's actual face, and does not extend to the application of facial-recognition technology to photographs, *Rivera* misconstrued BIPA's legislative history. Specifically, the court ascribed no significance to the fact that the General Assembly had considered and *rejected* a version of BIPA that would have included "facial recognition" in the definition of biometric identifier." *See* pp. 9-10 *supra*. The court found "no legislative explanation of *why* the term was dropped," and concluded that it may have been dropped "simply because it was redundant with 'facial geometry.'" 238 F. Supp. 3d at 1100. But that simply presumes the conclusion that "facial recognition" is the same thing as a "scan of facial geometry." The fact that the legislature consciously kept one term (although replacing "facial" with "face") and dropped the other is good evidence that *it* did not believe they were identical.

***Monroy.*** In the second iteration of this suit, Judge Gottschall rejected Shutterfly's argument for reasons that largely echoed *Rivera*'s analysis. *Monroy*, 2017 WL 4099846, at *2-5. We submit that the Court should not follow this decision for the same reasons it should not follow *Rivera*. And *Monroy* made two additional errors.

First, *Monroy* rejected Shutterfly's argument that, "by excluding data derived from photographs from the definition of 'biometric information,' the Illinois legislature intended to exclude from BIPA's purview all biometric data obtained from photographs." *Id.* at *3. The

court found this reading "problematic" because, "if biometric identifiers do not include information obtained from images or photographs, the definition's reference to a 'scan of face geometry' can "mean only an *in-person* scan of a person's face," and there is no "textual support for [that] interpretation." *Id.* This analysis is both circular and incorrect. It is circular because the principal "textual support" for the proposition that a "scan of face geometry" is limited to in-person scans is the very fact that the legislature expressly excluded information derived from *photos* from the purview of the statute. And it is incorrect because there is additional, independent textual support: the surrounding terms, all of which refer to an in-person collection of biometric data. *See* pp. 7-8 *supra.*

Second, *Monroy* found that "it appears that fingerprints and retinal scans can be obtained from images and photographs," citing articles suggesting that hackers can *fake* iris scans and fingerprints by "analyzing photographs." 2017 WL 4099846, at *4. But the legislature was not targeting the creation of *fake* biometric data; it was regulating the collection and storage of certain categories of *real* biometric data used for "financial transactions and security screenings."

In short, although several courts have rejected the arguments we make here, we respectfully submit that these decisions were mistaken because they did not sufficiently account for BIPA's text, structure, and legislative history. This Court should not follow these decisions, and it should hold that Shutterfly's technology is not covered by the statute.

## II. AT MINIMUM, THE COURT SHOULD DISMISS PLAINTIFFS' ALLEGATION THAT SHUTTERFLY DISSEMINATES BIOMETRIC DATA.

Separate from its notice-and-consent provisions, BIPA provides that no entity in possession of biometric data may "sell, lease, trade, or otherwise profit from" the data, and that it may not "disclose . . . or otherwise disseminate" the data without consent. 740 ILCS 14/15(c)-(d). Plaintiffs never mention these provisions, but they do briefly allege that, "[u]pon

information and belief, Shutterfly is selling, leasing, trading, or otherwise profiting from Plaintiffs' and Class members' biometric identifiers and/or biometric information." Compl. ¶ 48.

Shutterfly does *not* sell, lease, trade, or otherwise profit from or disseminate any data that is derived from, or otherwise connected with, its use of facial recognition technology. And plaintiffs do not allege with any specificity that it does. Rather, they allege only that Shutterfly uses facial-recognition technology to put people "in groups to make it fast and easy for [people] to tag" those groups. Compl. ¶ 21. Because plaintiffs never even cite the portions of BIPA governing the sale and dissemination of biometric data, they have not adequately alleged any claims based on those provisions. *See Roake v. Forest Preserve Dist. of Cook Cty.*, 2016 WL 3521895, at *3 (N.D. Ill. June 28, 2016) (cause of action failed because plaintiff did not "invoke" the relevant "statutory provision"—"[i]t is counsel's job, not the Court's, to construct a coherent complaint for the Plaintiff"). It is well-established that "conclusory, factually unsupported allegations" made only "[u]pon information and belief" must be "rejected." *Haywood v. Wexford Health Sources*, 2017 WL 783000, at *4 (N.D. Ill. Mar. 1, 2017); *see also Asset Allocation & Mgmt. Co. v. W. Emps. Ins. Co.*, 1989 WL 39728, at *5 (N.D. Ill. Apr. 19, 1989) (a "conclusory allegation . . . devoid of any factual allegations and based 'upon information and belief,' is insufficient."); *Autotech Techs. Ltd. P'ship v. Automationdirect.com, Inc.*, 237 F.R.D. 405, 412 (N.D. Ill. Aug. 21, 2006) (rejecting "conclusory allegation" "made upon information and belief" due to "absence of any explanation of the basis" for the allegation). Plaintiffs provide *no* factual allegations to support their claim that Shutterfly sells or disseminates their data. Therefore, the Court should strike plaintiffs' allegations of disclosure and sale and dismiss the complaint to the extent it is based on 740 ILCS 14/15(c)-(e).

## CONCLUSION

The Court should dismiss the complaint with prejudice.

DATED: October 3, 2019

Respectfully submitted,

By: */s/ Lauren R. Goldman*

MAYER BROWN LLP
Lauren R. Goldman
Michael Rayfield*
1221 Avenue of the Americas
New York, NY 10020
Telephone: (212) 506-2647
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

John Nadolenco*
350 South Grand Avenue
25th Floor
Los Angeles, CA 90071
Telephone: (213) 229-9500
jnadolenco@mayerbrown.com

Matthew D. Provance
71 S. Wacker Drive
Chicago, IL 60606
mprovance@mayerbrown.com
Telephone: (312) 782-0600

*Attorneys for Defendant Shutterfly, Inc.*

**CERTIFICATE OF SERVICE**

I hereby certify that on the 3rd day of October 2019, a copy of the foregoing Memorandum of Law in Support of Defendant's Motion to Dismiss was filed electronically and served by mail on anyone unable to accept electronic filing. Parties may access this filing through the court's CM/ECF System.

*/s/ Lauren R. Goldman* _____
Lauren R. Goldman
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
Tel: (212) 506-2373
Fax: (212) 849-5973
Email: lrgoldman@mayerbrown.com